Differential Equivalences on SBoxes

Valentin Suder, Christina Boura, Anne Canteaut, Jérémy Jean

Differential Equivalences on SBoxes

Valentin SUDER
(Université Rouen Normandie, France)

Joint work with Christina BOURA (UVSQ), Anne CANTEAUT (inria Paris, France) and Jérémy JEAN (ANSSI, France)

CAEN2018, Cryptography and Algorithmic Number Theory
June 21, 2018

Outline

Introduction
- Symmetric cryptography
- Differentiality
- Equivalences

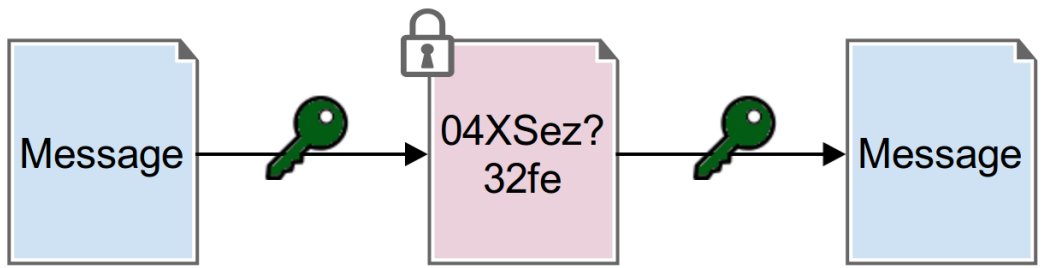
Results
- Equivalences
- Main contributions
- First Step for a classification
- Algorithm
- Experimental Results
- Special case

Conclusion

Symmetric Cryptography

Symmetric Cryptography

Cryptographic algorithms and protocols where the secret is **identical** between communicating parties.



- **Block ciphers**
- Stream ciphers
- Hash functions

Design of Block ciphers

Block cipher

A **block cipher** is a function

$$\begin{array}{rccc} E & : & \mathbb{F}_2^\kappa \times \mathbb{F}_2^m & \to & \mathbb{F}_2^m \\ & & (k, P) & \mapsto & C = E(k, P) := E_k(P) \end{array}$$

such that for any **fixed key** $k \in \mathbb{F}_2^\kappa$, E_k is *bijective* over $\mathbb{F}_2^m$.

Problem?

Design of Block ciphers

Block cipher

A **block cipher** is a function

$$\begin{array}{rccc} E & : & \mathbb{F}_2^\kappa \times \mathbb{F}_2^m & \to & \mathbb{F}_2^m \\ & & (k, P) & \mapsto & C = E(k, P) := E_k(P) \end{array}$$

such that for any **fixed key** $k \in \mathbb{F}_2^\kappa$, E_k is *bijective* over $\mathbb{F}_2^m$.

Problem? Usually, a block cipher is a set of 2^{80} permutations of $\mathbb{S}_{2^{128}}$.

Design of Block ciphers

Block cipher

A **block cipher** is a function

$$\begin{array}{rccc} E & : & \mathbb{F}_2^\kappa \times \mathbb{F}_2^m & \to & \mathbb{F}_2^m \\ & & (k, P) & \mapsto & C = E(k, P) := E_k(P) \end{array}$$

such that for any **fixed key** $k \in \mathbb{F}_2^\kappa$, E_k is *bijective* over $\mathbb{F}_2^m$.

Problem? Usually, a block cipher is a set of 2^{80} permutations of $\mathbb{S}_{2^{128}}$.

Solution: *Iterative construction*

$$E_k = R_{\ell-1} \circ R_{\ell-2} \circ \cdots \circ R_1 \circ \underbrace{R_0}_{\mathtt{L} \circ \mathtt{SB} \circ \mathtt{Add}_{k_0}},$$

Design of Block ciphers

Block cipher

A **block cipher** is a function

$$\begin{array}{rccc} E & : & \mathbb{F}_2^\kappa \times \mathbb{F}_2^m & \to & \mathbb{F}_2^m \\ & & (k, P) & \mapsto & C = E(k, P) := E_k(P) \end{array}$$

such that for any **fixed key** $k \in \mathbb{F}_2^\kappa$, E_k is *bijective* over $\mathbb{F}_2^m$.

Problem? Usually, a block cipher is a set of 2^{80} permutations of $\mathbb{S}_{2^{128}}$.

Solution: *Iterative construction*

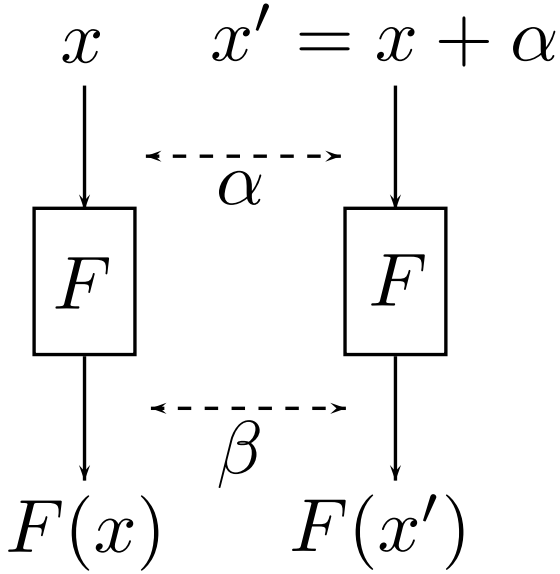
$$E_k = R_{\ell-1} \circ R_{\ell-2} \circ \cdots \circ R_1 \circ \underbrace{R_0}_{\mathtt{L} \circ \mathtt{SB} \circ \mathtt{Add}_{k_0}},$$

$$\begin{array}{rccc} \mathtt{SB} & : & \mathbb{F}_2^m = \mathbb{F}_2^n \times \mathbb{F}_2^n \times \ldots & \to & \mathbb{F}_2^m = \mathbb{F}_2^n \times \mathbb{F}_2^n \times \ldots \\ & & X = (x_0, x_1, \ldots) & \mapsto & (F_0(x_0), F_1(x_1), \ldots) \end{array}$$

Functions F_i's are usually called *SBoxes*.

Differential Criteria

$F : \mathbb{F}_2^n \to \mathbb{F}_2^n$



Derivatives in direction $\alpha \in \mathbb{F}_2^n$

$$\begin{array}{rccc} \Delta_\alpha F : & \mathbb{F}_2^n & \to & \mathbb{F}_2^n \\ & x & \mapsto & F(x) + F(x+\alpha) \end{array}$$

Differential Uniformity [Nyberg 94]

$$\delta_F = \max_{\alpha \in \mathbb{F}_2^n \setminus \{0\}, \beta \in \mathbb{F}_2^n} \#\{x \mid \Delta_\alpha F(x) = \beta\}$$

Whenever $\delta_F = 2$ (**minimal** value), the function F is said to be **APN** ('Almost Perfect Nonlinear').

Example

Differences Distribution Table (DDT)

Table of size $2^n \times 2^n$, with entries:

$$\mathcal{D}_F(\alpha, \beta) = \#\left\{x \in \mathbb{F}_2^n \mid \Delta_\alpha F(x) = \beta\right\}, \forall \alpha, \beta \in \mathbb{F}_2^n.$$

	$\mathcal{D}_F$	β							
		0	1	2	3	4	5	6	7
	0	8	.	.	.	.	.	.	.
	1	.	2	.	2	.	2	.	2
	2	.	.	2	2	.	.	2	2
α	3	.	2	2	.	.	2	2	.
	4	.	.	.	.	2	2	2	2
	5	.	2	.	2	2	.	2	.
	6	.	.	2	2	2	2	.	.
	7	.	2	2	.	2	.	.	2

	$\mathcal{D}_{F'}$	β							
		0	1	2	3	4	5	6	7
	0	8	.	.	.	.	.	.	.
	1	.	.	8	.	.	.	.	.
	2	.	.	.	4	.	.	4	.
	3	.	2	.	.	6	.	.	.
	4	.	.	.	.	2	.	2	4
	5	.	2	.	2	.	.	2	2
	6	.	2	.	2	.	4	.	.
	7	.	2	.	.	.	4	.	2

Big APN Problem

APN functions $\Rightarrow$ Best resistance to **differential cryptanalysis**!

1. **Very few** known APN functions . . .
2. . . . even fewer known bijective APN functions (none when $n = 4$)

'Big APN Problem' :
Is there any **bijective APN functions** over $\mathbb{F}_{2^n}$, when n is **even** ?

Answer (?) : In 2009, Dillon et al. found only one example for $n = 6$. Since then, **nothing more** (or very little) . . .

3. **Few** (bijective) functions are known with $\delta = 4$.

K. A. Browning, J. F. Dillon, M. T. McQuistan and A. J. Wolfe,
An APN Permutation in Dimension Six,
Fq9 (Selected Papers), Contemporary Mathematics, 2010.

Some equivalence classes

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$

The **differential uniformity** $\delta(F)$ of F is an invariant under:

- compositional inverse (if F is bijective): $\delta(F^{-1}) = \delta(F)$

Some equivalence classes

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$

The **differential uniformity** $\delta(F)$ of F is an invariant under:

- compositional inverse (if F is bijective): $\delta(F^{-1}) = \delta(F)$
- affine permutations: $\delta(F) = \delta(A_1 \circ F \circ A_2 + A')$

  $\Rightarrow$ **EA-equivalence** $(\sim_{EA})$

Some equivalence classes

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$

The **differential uniformity** $\delta(F)$ of F is an invariant under:

- compositional inverse (if F is bijective): $\delta(F^{-1}) = \delta(F)$
- affine permutations: $\delta(F) = \delta(A_1 \circ F \circ A_2 + A')$
  $\Rightarrow$ **EA-equivalence** $(\sim_{EA})$
- Graph equivalence: $\mathcal{G}_{F'} = \{\mathcal{L}(x, F(x))\} = \mathcal{L}(\mathcal{G}_F)$, $\delta(F) = \delta(F')$
  $\Rightarrow$ **CCZ-equivalence** $(\sim_{CCZ})$

$$\mathcal{MG}_F = \begin{pmatrix} | & & | & & | \\ 1 & \dots & x & \dots & 2^n - 1 \\ | & & | & & | \\ | & & | & & | \\ F(1) & \dots & F(x) & \dots & F(2^n - 1) \\ | & & | & & | \end{pmatrix}$$

Some equivalence classes

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$

The **differential uniformity** $\delta(F)$ of F is an invariant under:

- compositional inverse (if F is bijective): $\delta(F^{-1}) = \delta(F)$
- affine permutations: $\delta(F) = \delta(A_1 \circ F \circ A_2 + A')$
  $\Rightarrow$ **EA-equivalence** $(\sim_{EA})$
- Graph equivalence: $\mathcal{G}_{F'} = \{\mathcal{L}(x, F(x))\} = \mathcal{L}(\mathcal{G}_F)$, $\delta(F) = \delta(F')$
  $\Rightarrow$ **CCZ-equivalence** $(\sim_{CCZ})$

$$\mathcal{MG}_F = \begin{pmatrix} | & & | & & | \\ 1 & \dots & x & \dots & 2^n - 1 \\ | & & | & & | \\ | & & | & & | \\ F(1) & \dots & F(x) & \dots & F(2^n - 1) \\ | & & | & & | \end{pmatrix}$$

EA-Eq $\overset{\Rightarrow}{\not\Leftarrow}$ **CCZ-Eq**

Link with other areas

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$

Carlet-Charpin-Zinoviev (1998)

F is APN **if and only if** the minimal distance of the linear code with parity check matrix $\mathcal{MG}_F$ is 5.

Link with other areas

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$

Carlet-Charpin-Zinoviev (1998)

F is APN **if and only if** the minimal distance of the linear code with parity check matrix $\mathcal{MG}_F$ is 5.

Coulter-Henderson (1999)

If F is APN **then** the **incidence structure** of $\mathcal{G}_F$ is a $(2^{2n}, 2^n)$-semibiplane.

Link with other areas

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$

Carlet-Charpin-Zinoviev (1998)

F is APN **if and only if** the minimal distance of the linear code with parity check matrix $\mathcal{MG}_F$ is 5.

Coulter-Henderson (1999)

If F is APN **then** the **incidence structure** of $\mathcal{G}_F$ is a $(2^{2n}, 2^n)$-semibiplane.

Let F be **quadratic**, i.e. $F(x) = \sum_{i,j} c_{i,j} x^{2^i+2^j} \in \mathbb{F}_{2^n}[x]$.

F APN $\Rightarrow$ semifields, dual hyperoval, rank-metric code,...

$\vdots$

Link with other areas

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$

Carlet-Charpin-Zinoviev (1998)

F is APN **if and only if** the minimal distance of the linear code with parity check matrix $\mathcal{MG}_F$ is 5.

Coulter-Henderson (1999)

If F is APN **then** the **incidence structure** of $\mathcal{G}_F$ is a $(2^{2n}, 2^n)$-semibiplane.

Let F be **quadratic**, i.e. $F(x) = \sum_{i,j} c_{i,j} x^{2^i+2^j} \in \mathbb{F}_{2^n}[x]$.

F APN $\Rightarrow$ semifields, dual hyperoval, rank-metric code,...

$\vdots$

not only **cryptography** benefits from research on **APN functions**.

Outline

Introduction
- Symmetric cryptography
- Differentiality
- Equivalences

Results
- Equivalences
- Main contributions
- First Step for a classification
- Algorithm
- Experimental Results
- Special case

Conclusion

Differential equivalences of SBoxes

$F, G : \mathbb{F}_2^n \to \mathbb{F}_2^n$

Definitions :

Differences Distribution Table (DDT)

Table of size $2^n \times 2^n$, with entries:

$$\mathcal{D}_F(\alpha, \beta) = \#\left\{x \in \mathbb{F}_2^n \mid \Delta_\alpha F(x) = \beta\right\}, \forall \alpha, \beta \in \mathbb{F}_2^n.$$

Indicator of a DDT

Boolean function $\gamma_F : \mathbb{F}_2^{n \times n} \to \mathbb{F}_2$,

$$\gamma_F(\alpha, \beta) = 0 \Leftrightarrow \delta_F(\alpha, \beta) = 0 \text{ or } \alpha = 0.$$

Differential equivalences of SBoxes

$F, G : \mathbb{F}_2^n \to \mathbb{F}_2^n$

Definitions :

Differences Distribution Table (DDT)

Table of size $2^n \times 2^n$, with entries:

$$\mathcal{D}_F(\alpha, \beta) = \#\left\{x \in \mathbb{F}_2^n \mid \Delta_\alpha F(x) = \beta\right\}, \forall \alpha, \beta \in \mathbb{F}_2^n.$$

Indicator of a DDT

Boolean function $\gamma_F : \mathbb{F}_2^{n \times n} \to \mathbb{F}_2$,

$$\gamma_F(\alpha, \beta) = 0 \Leftrightarrow \delta_F(\alpha, \beta) = 0 \text{ or } \alpha = 0.$$

$\Rightarrow$ Two **equivalences**:

- $F \sim_{\mathcal{D}} G \quad \Leftrightarrow \quad \mathcal{D}_F = \mathcal{D}_G,$
- $F \sim_{\gamma} G \quad \Leftrightarrow \quad \gamma_F = \gamma_G.$

Motivation, Origin

Differential Equivalence

In **odd** characteristic, Perfect Nonlinear (PN) functions are such that all of their derivatives are **bijective** $\Rightarrow$ all PN functions have the same DDT.

Gorodilova introduced the γ-equivalence, while working on **APN monomial quadratic** functions (aka **Gold** functions, aka APN functions of the type $x \mapsto x^{2^i+1}$).

A Gorodilova,
On a remarkable property of APN Gold functions,
Cryptology ePrint Archive, 2016.

Examples

n=4

$$F = [0,1,2,3,4,5,6,7,8,9,10,11,12,13,15,14],$$
$$G = [0,1,3,2,5,4,7,6,8,9,10,11,12,13,14,15].$$

$$\mathcal{D}_F = \begin{bmatrix}
16 & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . \\
. & 16 & . & . & . & . & . & . & . & . & . & . & . & . & . & . \\
. & . & 12 & 4 & . & . & . & . & . & . & . & . & . & . & . & . \\
. & . & 4 & 12 & . & . & . & . & . & . & . & . & . & . & . & . \\
. & . & . & . & 12 & 4 & . & . & . & . & . & . & . & . & . & . \\
. & . & . & . & 4 & 12 & . & . & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & 12 & 4 & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & 4 & 12 & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & 12 & 4 & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & 4 & 12 & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . & 12 & 4 & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . & 4 & 12 & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . & . & . & 12 & 4 & . & . \\
. & . & . & . & . & . & . & . & . & . & . & . & 4 & 12 & . & . \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . & 12 & 4 \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . & 4 & 12
\end{bmatrix}$$

Examples

n=4

$$F = [0,1,2,3,4,5,6,7,8,9,10,11,12,13,15,14],$$
$$G = [0,1,3,2,5,4,7,6,8,9,10,11,12,13,14,15].$$

$$\mathcal{D}_G = \begin{bmatrix}
16 & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . \\
. & 16 & . & . & . & . & . & . & . & . & . & . & . & . & . & . \\
. & . & 12 & 4 & . & . & . & . & . & . & . & . & . & . & . & . \\
. & . & 4 & 12 & . & . & . & . & . & . & . & . & . & . & . & . \\
. & . & . & . & 12 & 4 & . & . & . & . & . & . & . & . & . & . \\
. & . & . & . & 4 & 12 & . & . & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & 12 & 4 & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & 4 & 12 & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & 4 & 12 & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & 12 & 4 & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . & 4 & 12 & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . & 12 & 4 & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . & . & . & 4 & 12 & . & . \\
. & . & . & . & . & . & . & . & . & . & . & . & 12 & 4 & . & . \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . & 4 & 12 \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . & 12 & 4
\end{bmatrix} \neq \mathcal{D}_F$$

Examples

n=4

$$F = [0,1,2,3,4,5,6,7,8,9,10,11,12,13,15,14],$$
$$G = [0,1,3,2,5,4,7,6,8,9,10,11,12,13,14,15].$$

$\gamma_G =$

$$\begin{pmatrix}
0 & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . \\
. & 1 & . & . & . & . & . & . & . & . & . & . & . & . & . & . \\
. & . & 1 & 1 & . & . & . & . & . & . & . & . & . & . & . & . \\
. & . & 1 & 1 & . & . & . & . & . & . & . & . & . & . & . & . \\
. & . & . & . & 1 & 1 & . & . & . & . & . & . & . & . & . & . \\
. & . & . & . & 1 & 1 & . & . & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & 1 & 1 & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & 1 & 1 & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & 1 & 1 & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & 1 & 1 & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . & 1 & 1 & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . & 1 & 1 & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . & . & . & 1 & 1 & . & . \\
. & . & . & . & . & . & . & . & . & . & . & . & 1 & 1 & . & . \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . & 1 & 1 \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . & 1 & 1
\end{pmatrix}$$

Examples

n=4

$$F = [0,1,2,3,4,5,6,7,8,9,10,11,12,13,15,14],$$
$$G = [0,1,3,2,5,4,7,6,8,9,10,11,12,13,14,15].$$

$$\gamma_G = \begin{pmatrix}
0 & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . \\
. & 1 & . & . & . & . & . & . & . & . & . & . & . & . & . & . \\
. & . & 1 & 1 & . & . & . & . & . & . & . & . & . & . & . & . \\
. & . & 1 & 1 & . & . & . & . & . & . & . & . & . & . & . & . \\
. & . & . & . & 1 & 1 & . & . & . & . & . & . & . & . & . & . \\
. & . & . & . & 1 & 1 & . & . & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & 1 & 1 & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & 1 & 1 & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & 1 & 1 & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & 1 & 1 & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . & 1 & 1 & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . & 1 & 1 & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . & . & . & 1 & 1 & . & . \\
. & . & . & . & . & . & . & . & . & . & . & . & 1 & 1 & . & . \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . & 1 & 1 \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . & 1 & 1
\end{pmatrix} = \gamma_F$$

Properties

$F, G : \mathbb{F}_2^n \to \mathbb{F}_2^n$

Basic:

- $F \sim_{\mathcal{D}} G \quad \Rightarrow \quad F \sim_{\gamma} G \quad (\not\Leftarrow)$
- for any $a, b \in \mathbb{F}_2^n$,

$$F(x) \sim_{\mathcal{D}} G(x) = F(x + a) + b$$

in that case, F and G are said to be **trivially equivalent**.

A little more advanced:

- if F and G are either **APN** or **quadratic** (or both), then

$$F \sim_{\mathcal{D}} G \quad \Leftrightarrow \quad F \sim_{\gamma} G$$

What are the functions that share the same **DDT**?
the same **indicator**? How many of them exist?

What are the functions that share the same **DDT**? the same **indicator**? How many of them exist?

Contributions :

- Using **EA-Eq** and **CCZ-Eq** to *help* the classification
- a **recursive algorithm** to compute equivalence classes.
  Input : a DDT (resp. indicator),
  Output : **every functions** having this DDT (resp. indicator)
- **research** for some known functions.
- **new fact** about APN permutations.

C. Boura, A. Canteaut, J. Jean and V. Suder,
Two Notions of Differential Equivalence on SBoxes,
DCC, Design, Codes and Cryptography, To appear.

Relation to CCZ-Eq and EA-Eq

Gorodilova (2016)

For $F \sim_{EA} G$,

$$\forall\ F' \sim_{\gamma} F \Rightarrow \exists\ G' \sim_{\gamma} G \text{ s.t. } G' \sim_{EA} F'$$

Relation to CCZ-Eq and EA-Eq

Gorodilova (2016)

For $F \sim_{EA} G$,

$$\forall\ F' \sim_{\gamma} F \Rightarrow \exists\ G' \sim_{\gamma} G \text{ s.t. } G' \sim_{EA} F'$$

Boura-Canteaut-Jean-S. [WCC'17]

For $F \sim_{EA} G$,

$$\forall\ F' \sim_{DDT} F \Rightarrow \exists\ G' \sim_{DDT} G \text{ s.t. } G' \sim_{EA} F'$$

Relation to CCZ-Eq and EA-Eq

Gorodilova (2016)

For $F \sim_{EA} G$,

$$\forall\ F' \sim_{\gamma} F \Rightarrow \exists\ G' \sim_{\gamma} G \text{ s.t. } G' \sim_{EA} F'$$

Boura-Canteaut-Jean-S. [WCC'17]

For $F \sim_{EA} G$,

$$\forall\ F' \sim_{DDT} F \Rightarrow \exists\ G' \sim_{DDT} G \text{ s.t. } G' \sim_{EA} F'$$

Boura-Canteaut-Jean-S. [DCC]

For $F \sim_{CCZ} G$,

$$\forall\ F' \sim_{DDT} F \Rightarrow \exists\ G' \sim_{DDT} G \text{ s.t. } G' \sim_{CCZ} F'$$

Overview

Input : a DDT (resp. indicator),
Output : **every functions** having this DDT (resp. indicator)

Idea: Recursive Tree-traversal algorithm

Overview

Input : a DDT (resp. indicator),
Output : **every functions** having this DDT (resp. indicator)

Idea: Recursive Tree-traversal algorithm

- Tree of depth 2^n, each nodes at a level i corresponds to one **possible value** for $F(i)$

Overview

Input : a DDT (resp. indicator),
Output : **every functions** having this DDT (resp. indicator)

Idea: Recursive Tree-traversal algorithm

- Tree of depth 2^n, each nodes at a level i corresponds to one **possible value** for $F(i)$
- From the constraints of the DDT and the values $F(0), \ldots, F(i-1)$:
  - find **all possible values** for $F(i)$
  - **for each** of them, move on to the next step $F(i+1)$, and **backtrack** if necessary

Overview

Input : a DDT (resp. indicator),
Output : **every functions** having this DDT (resp. indicator)

Idea: Recursive Tree-traversal algorithm

- Tree of depth 2^n, each nodes at a level i corresponds to one **possible value** for $F(i)$
- From the constraints of the DDT and the values $F(0), \ldots, F(i-1)$:
  - find **all possible values** for $F(i)$
  - **for each** of them, move on to the next step $F(i+1)$, and **backtrack** if necessary

Pruning trick: We can **fix** $F(0)$ and $F(1)$:

$$G(x+1) + G(1) := F(x) \sim_{\mathcal{D}} G(x)$$

so that

$$F(0) = 0, \quad \text{and } F(1) = \Delta_1 F(0) = \Delta_1 G(0)$$

Example

$\mathbb{F}_2^3$

$$\mathcal{R}_i := \{j \mid \mathcal{D}(i,j) \neq 0\}$$

$\mathcal{D}$	0	1	2	3	4	5	6	7
0	8	.	.	.	.	.	.	.
1	.	2	.	2	.	2	.	2
2	.	.	2	2	.	.	2	2
3	.	2	2	.	.	2	2	.
4	.	.	.	.	2	2	2	2
5	.	2	.	2	2	.	2	.
6	.	.	2	2	2	2	.	.
7	.	2	2	.	2	.	.	2

0. Set $F(0) = 0$

Example

$\mathbb{F}_2^3$

$$\mathcal{R}_i := \{j \mid \mathcal{D}(i,j) \neq 0\}$$

$\mathcal{D}$	0	1	2	3	4	5	6	7
0	8	.	.	.	.	.	.	.
1	.	2	.	2	.	2	.	2
2	.	.	2	2	.	.	2	2
3	.	2	2	.	.	2	2	.
4	.	.	.	.	2	2	2	2
5	.	2	.	2	2	.	2	.
6	.	.	2	2	2	2	.	.
7	.	2	2	.	2	.	.	2

0. Set $F(0) = 0$
1. $F(0) + F(1) \in \mathcal{R}_1 = \{1, 3, 5, 7\}$
   Set $F(1) = 1$

Example

$\mathbb{F}_2^3$

$$\mathcal{R}_i := \{j \mid \mathcal{D}(i,j) \neq 0\}$$

$\mathcal{D}$	0	1	2	3	4	5	6	7
0	8	.	.	.	.	.	.	.
1	.	2	.	2	.	2	.	2
2	.	.	2	2	.	.	2	2
3	.	2	2	.	.	2	2	.
4	.	.	.	.	2	2	2	2
5	.	2	.	2	2	.	2	.
6	.	.	2	2	2	2	.	.
7	.	2	2	.	2	.	.	2

0. Set $F(0) = 0$
1. $F(0) + F(1) \in \mathcal{R}_1 = \{1, 3, 5, 7\}$
   Set $F(1) = 1$
2. $F(0) + F(2) \in \mathcal{R}_2 = \{2, 3, 6, 7\}$

Example

$\mathbb{F}_2^3$

$$\mathcal{R}_i := \{j \mid \mathcal{D}(i,j) \neq 0\}$$

$\mathcal{D}$	0	1	2	3	4	5	6	7
0	8	.	.	.	.	.	.	.
1	.	2	.	2	.	2	.	2
2	.	.	2	2	.	.	2	2
3	.	2	2	.	.	2	2	.
4	.	.	.	.	2	2	2	2
5	.	2	.	2	2	.	2	.
6	.	.	2	2	2	2	.	.
7	.	2	2	.	2	.	.	2

0. Set $F(0) = 0$
1. $F(0) + F(1) \in \mathcal{R}_1 = \{1, 3, 5, 7\}$
   Set $F(1) = 1$
2. $F(0) + F(2) \in \mathcal{R}_2 = \{2, 3, 6, 7\}$ and
   $F(1) + F(2) \in \mathcal{R}_3 = \{1, 2, 5, 6\}$

Example

$\mathbb{F}_2^3$

$$\mathcal{R}_i := \{j \mid \mathcal{D}(i,j) \neq 0\}$$

$\mathcal{D}$	0	1	2	3	4	5	6	7
0	8	.	.	.	.	.	.	.
1	.	2	.	2	.	2	.	2
2	.	.	2	2	.	.	2	2
3	.	2	2	.	.	2	2	.
4	.	.	.	.	2	2	2	2
5	.	2	.	2	2	.	2	.
6	.	.	2	2	2	2	.	.
7	.	2	2	.	2	.	.	2

0. Set $F(0) = 0$
1. $F(0) + F(1) \in \mathcal{R}_1 = \{1, 3, 5, 7\}$
   Set $F(1) = 1$
2. $F(0) + F(2) \in \mathcal{R}_2 = \{2, 3, 6, 7\}$ and
   $F(1) + F(2) \in \mathcal{R}_3 = \{1, 2, 5, 6\}$ thus

   $F(2) \in F(0)+\mathcal{R}_1 \cap F(1)+\mathcal{R}_3 = \{3, 7\}$

Example

$\mathbb{F}_2^3$

$$\mathcal{R}_i := \{j \mid \mathcal{D}(i,j) \neq 0\}$$

$\mathcal{D}$	0	1	2	3	4	5	6	7
0	8	.	.	.	.	.	.	.
1	.	2	.	2	.	2	.	2
2	.	.	2	2	.	.	2	2
3	.	2	2	.	.	2	2	.
4	.	.	.	.	2	2	2	2
5	.	2	.	2	2	.	2	.
6	.	.	2	2	2	2	.	.
7	.	2	2	.	2	.	.	2

0. Set $F(0) = 0$
1. $F(0) + F(1) \in \mathcal{R}_1 = \{1, 3, 5, 7\}$
   Set $F(1) = 1$
2. $F(0) + F(2) \in \mathcal{R}_2 = \{2, 3, 6, 7\}$ and
   $F(1) + F(2) \in \mathcal{R}_3 = \{1, 2, 5, 6\}$ thus

   $F(2) \in F(0)+\mathcal{R}_1 \cap F(1)+\mathcal{R}_3 = \{3, 7\}$
3. $F(0) + F(3) \in \mathcal{R}_3 = \{1, 2, 5, 6\}$

Example

$\mathbb{F}_2^3$

$$\mathcal{R}_i := \{j \mid \mathcal{D}(i,j) \neq 0\}$$

$\mathcal{D}$	0	1	2	3	4	5	6	7
0	8	.	.	.	.	.	.	.
1	.	2	.	2	.	2	.	2
2	.	.	2	2	.	.	2	2
3	.	2	2	.	.	2	2	.
4	.	.	.	.	2	2	2	2
5	.	2	.	2	2	.	2	.
6	.	.	2	2	2	2	.	.
7	.	2	2	.	2	.	.	2

0. Set $F(0) = 0$
1. $F(0) + F(1) \in \mathcal{R}_1 = \{1, 3, 5, 7\}$
   Set $F(1) = 1$
2. $F(0) + F(2) \in \mathcal{R}_2 = \{2, 3, 6, 7\}$ and
   $F(1) + F(2) \in \mathcal{R}_3 = \{1, 2, 5, 6\}$ thus

   $F(2) \in F(0) + \mathcal{R}_1 \cap F(1) + \mathcal{R}_3 = \{3, 7\}$
3. $F(0) + F(3) \in \mathcal{R}_3 = \{1, 2, 5, 6\}$ and
   $F(1) + F(3) \in \mathcal{R}_2 = \{2, 3, 6, 7\}$

Example

$\mathbb{F}_2^3$

$$\mathcal{R}_i := \{j \mid \mathcal{D}(i,j) \neq 0\}$$

$\mathcal{D}$	0	1	2	3	4	5	6	7
0	8	.	.	.	.	.	.	.
1	.	2	.	2	.	2	.	2
2	.	.	2	2	.	.	2	2
3	.	2	2	.	.	2	2	.
4	.	.	.	.	2	2	2	2
5	.	2	.	2	2	.	2	.
6	.	.	2	2	2	2	.	.
7	.	2	2	.	2	.	.	2

0. Set $F(0) = 0$
1. $F(0) + F(1) \in \mathcal{R}_1 = \{1, 3, 5, 7\}$
   Set $F(1) = 1$
2. $F(0) + F(2) \in \mathcal{R}_2 = \{2, 3, 6, 7\}$ and
   $F(1) + F(2) \in \mathcal{R}_3 = \{1, 2, 5, 6\}$ thus

   $F(2) \in F(0) + \mathcal{R}_1 \cap F(1) + \mathcal{R}_3 = \{3, 7\}$
3. $F(0) + F(3) \in \mathcal{R}_3 = \{1, 2, 5, 6\}$ and
   $F(1) + F(3) \in \mathcal{R}_2 = \{2, 3, 6, 7\}$ and
   $F(2) + F(3) \in \mathcal{R}_1 = \{1, 3, 5, 7\}$

Example

$\mathbb{F}_2^3$

$$\mathcal{R}_i := \{j \mid \mathcal{D}(i,j) \neq 0\}$$

$\mathcal{D}$	0	1	2	3	4	5	6	7
0	8	.	.	.	.	.	.	.
1	.	2	.	2	.	2	.	2
2	.	.	2	2	.	.	2	2
3	.	2	2	.	.	2	2	.
4	.	.	.	.	2	2	2	2
5	.	2	.	2	2	.	2	.
6	.	.	2	2	2	2	.	.
7	.	2	2	.	2	.	.	2

0. Set $F(0) = 0$
1. $F(0) + F(1) \in \mathcal{R}_1 = \{1, 3, 5, 7\}$
   Set $F(1) = 1$
2. $F(0) + F(2) \in \mathcal{R}_2 = \{2, 3, 6, 7\}$ and
   $F(1) + F(2) \in \mathcal{R}_3 = \{1, 2, 5, 6\}$ thus

   $F(2) \in F(0) + \mathcal{R}_1 \cap F(1) + \mathcal{R}_3 = \{3, 7\}$
3. $F(0) + F(3) \in \mathcal{R}_3 = \{1, 2, 5, 6\}$ and
   $F(1) + F(3) \in \mathcal{R}_2 = \{2, 3, 6, 7\}$ and
   $F(2) + F(3) \in \mathcal{R}_1 = \{1, 3, 5, 7\}$ thus

   $F(3) \in \{2, 6\}$ (**OR** $\{2, 6\}$)

Example

$\mathbb{F}_2^3$

$$\mathcal{R}_i := \{j \mid \mathcal{D}(i,j) \neq 0\}$$

$\mathcal{D}$	0	1	2	3	4	5	6	7
0	8	.	.	.	.	.	.	.
1	.	2	.	2	.	2	.	2
2	.	.	2	2	.	.	2	2
3	.	2	2	.	.	2	2	.
4	.	.	.	.	2	2	2	2
5	.	2	.	2	2	.	2	.
6	.	.	2	2	2	2	.	.
7	.	2	2	.	2	.	.	2

0. Set $F(0) = 0$
1. $F(0) + F(1) \in \mathcal{R}_1 = \{1, 3, 5, 7\}$
   Set $F(1) = 1$
2. $F(0) + F(2) \in \mathcal{R}_2 = \{2, 3, 6, 7\}$ and
   $F(1) + F(2) \in \mathcal{R}_3 = \{1, 2, 5, 6\}$ thus

   $F(2) \in F(0) + \mathcal{R}_1 \cap F(1) + \mathcal{R}_3 = \{3, 7\}$
3. $F(0) + F(3) \in \mathcal{R}_3 = \{1, 2, 5, 6\}$ and
   $F(1) + F(3) \in \mathcal{R}_2 = \{2, 3, 6, 7\}$ and
   $F(2) + F(3) \in \mathcal{R}_1 = \{1, 3, 5, 7\}$ thus

   $F(3) \in \{2, 6\}$ (**OR** $\{2, 6\}$)
4. $F(0) + F(4) \in \mathcal{R}_4 = \{4, 5, 6, 7\}$

Example

$\mathbb{F}_2^3$

$$\mathcal{R}_i := \{j \mid \mathcal{D}(i,j) \neq 0\}$$

$\mathcal{D}$	0	1	2	3	4	5	6	7
0	8	.	.	.	.	.	.	.
1	.	2	.	2	.	2	.	2
2	.	.	2	2	.	.	2	2
3	.	2	2	.	.	2	2	.
4	.	.	.	.	2	2	2	2
5	.	2	.	2	2	.	2	.
6	.	.	2	2	2	2	.	.
7	.	2	2	.	2	.	.	2

0. Set $F(0) = 0$
1. $F(0) + F(1) \in \mathcal{R}_1 = \{1, 3, 5, 7\}$
   Set $F(1) = 1$
2. $F(0) + F(2) \in \mathcal{R}_2 = \{2, 3, 6, 7\}$ and
   $F(1) + F(2) \in \mathcal{R}_3 = \{1, 2, 5, 6\}$ thus

   $F(2) \in F(0) + \mathcal{R}_1 \cap F(1) + \mathcal{R}_3 = \{3, 7\}$
3. $F(0) + F(3) \in \mathcal{R}_3 = \{1, 2, 5, 6\}$ and
   $F(1) + F(3) \in \mathcal{R}_2 = \{2, 3, 6, 7\}$ and
   $F(2) + F(3) \in \mathcal{R}_1 = \{1, 3, 5, 7\}$ thus

   $F(3) \in \{2, 6\}$ (**OR** $\{2, 6\}$)
4. $F(0) + F(4) \in \mathcal{R}_4 = \{4, 5, 6, 7\}$ and
   $F(1) + F(4) \in \mathcal{R}_5 = \{1, 3, 4, 6\}$

Example

$\mathbb{F}_2^3$

$$\mathcal{R}_i := \{j \mid \mathcal{D}(i,j) \neq 0\}$$

$\mathcal{D}$	0	1	2	3	4	5	6	7
0	8	.	.	.	.	.	.	.
1	.	2	.	2	.	2	.	2
2	.	.	2	2	.	.	2	2
3	.	2	2	.	.	2	2	.
4	.	.	.	.	2	2	2	2
5	.	2	.	2	2	.	2	.
6	.	.	2	2	2	2	.	.
7	.	2	2	.	2	.	.	2

0. Set $F(0) = 0$
1. $F(0) + F(1) \in \mathcal{R}_1 = \{1, 3, 5, 7\}$
   Set $F(1) = 1$
2. $F(0) + F(2) \in \mathcal{R}_2 = \{2, 3, 6, 7\}$ and
   $F(1) + F(2) \in \mathcal{R}_3 = \{1, 2, 5, 6\}$ thus

   $F(2) \in F(0) + \mathcal{R}_1 \cap F(1) + \mathcal{R}_3 = \{3, 7\}$
3. $F(0) + F(3) \in \mathcal{R}_3 = \{1, 2, 5, 6\}$ and
   $F(1) + F(3) \in \mathcal{R}_2 = \{2, 3, 6, 7\}$ and
   $F(2) + F(3) \in \mathcal{R}_1 = \{1, 3, 5, 7\}$ thus

   $F(3) \in \{2, 6\}$ (**OR** $\{2, 6\}$)
4. $F(0) + F(4) \in \mathcal{R}_4 = \{4, 5, 6, 7\}$ and
   $F(1) + F(4) \in \mathcal{R}_5 = \{1, 3, 4, 6\}$ and
   $F(2) + F(4) \in \mathcal{R}_6 = \{2, 3, 4, 5\}$

Example

$\mathbb{F}_2^3$

$$\mathcal{R}_i := \{j \mid \mathcal{D}(i,j) \neq 0\}$$

$\mathcal{D}$	0	1	2	3	4	5	6	7
0	8	.	.	.	.	.	.	.
1	.	2	.	2	.	2	.	2
2	.	.	2	2	.	.	2	2
3	.	2	2	.	.	2	2	.
4	.	.	.	.	2	2	2	2
5	.	2	.	2	2	.	2	.
6	.	.	2	2	2	2	.	.
7	.	2	2	.	2	.	.	2

0. Set $F(0) = 0$
1. $F(0) + F(1) \in \mathcal{R}_1 = \{1, 3, 5, 7\}$
   Set $F(1) = 1$
2. $F(0) + F(2) \in \mathcal{R}_2 = \{2, 3, 6, 7\}$ and
   $F(1) + F(2) \in \mathcal{R}_3 = \{1, 2, 5, 6\}$ thus

   $F(2) \in F(0) + \mathcal{R}_1 \cap F(1) + \mathcal{R}_3 = \{3, 7\}$
3. $F(0) + F(3) \in \mathcal{R}_3 = \{1, 2, 5, 6\}$ and
   $F(1) + F(3) \in \mathcal{R}_2 = \{2, 3, 6, 7\}$ and
   $F(2) + F(3) \in \mathcal{R}_1 = \{1, 3, 5, 7\}$ thus

   $F(3) \in \{2, 6\}$ (**OR** $\{2, 6\}$)
4. $F(0) + F(4) \in \mathcal{R}_4 = \{4, 5, 6, 7\}$ and
   $F(1) + F(4) \in \mathcal{R}_5 = \{1, 3, 4, 6\}$ and
   $F(2) + F(4) \in \mathcal{R}_6 = \{2, 3, 4, 5\}$ and
   $F(3) + F(4) \in \mathcal{R}_7 = \{1, 2, 4, 7\}$

Example

$\mathbb{F}_2^3$

$$\mathcal{R}_i := \{j \mid \mathcal{D}(i,j) \neq 0\}$$

$\mathcal{D}$	0	1	2	3	4	5	6	7
0	8	.	.	.	.	.	.	.
1	.	2	.	2	.	2	.	2
2	.	.	2	2	.	.	2	2
3	.	2	2	.	.	2	2	.
4	.	.	.	.	2	2	2	2
5	.	2	.	2	2	.	2	.
6	.	.	2	2	2	2	.	.
7	.	2	2	.	2	.	.	2

0. Set $F(0) = 0$
1. $F(0) + F(1) \in \mathcal{R}_1 = \{1, 3, 5, 7\}$
   Set $F(1) = 1$
2. $F(0) + F(2) \in \mathcal{R}_2 = \{2, 3, 6, 7\}$ and
   $F(1) + F(2) \in \mathcal{R}_3 = \{1, 2, 5, 6\}$ thus

   $F(2) \in F(0) + \mathcal{R}_1 \cap F(1) + \mathcal{R}_3 = \{3, 7\}$
3. $F(0) + F(3) \in \mathcal{R}_3 = \{1, 2, 5, 6\}$ and
   $F(1) + F(3) \in \mathcal{R}_2 = \{2, 3, 6, 7\}$ and
   $F(2) + F(3) \in \mathcal{R}_1 = \{1, 3, 5, 7\}$ thus

   $F(3) \in \{2, 6\}$ (**OR** $\{2, 6\}$)
4. $F(0) + F(4) \in \mathcal{R}_4 = \{4, 5, 6, 7\}$ and
   $F(1) + F(4) \in \mathcal{R}_5 = \{1, 3, 4, 6\}$ and
   $F(2) + F(4) \in \mathcal{R}_6 = \{2, 3, 4, 5\}$ and
   $F(3) + F(4) \in \mathcal{R}_7 = \{1, 2, 4, 7\}$ thus

   $F(4) \in \{\emptyset\}$ **if** $F(2) = 3$ and $F(3) = 2$

Example

$\mathbb{F}_2^3$

$$\mathcal{R}_i := \{j \mid \mathcal{D}(i,j) \neq 0\}$$

$\mathcal{D}$	0	1	2	3	4	5	6	7
0	8	.	.	.	.	.	.	.
1	.	2	.	2	.	2	.	2
2	.	.	2	2	.	.	2	2
3	.	2	2	.	.	2	2	.
4	.	.	.	.	2	2	2	2
5	.	2	.	2	2	.	2	.
6	.	.	2	2	2	2	.	.
7	.	2	2	.	2	.	.	2

0. Set $F(0) = 0$
1. $F(0) + F(1) \in \mathcal{R}_1 = \{1, 3, 5, 7\}$
   Set $F(1) = 1$
2. $F(0) + F(2) \in \mathcal{R}_2 = \{2, 3, 6, 7\}$ and
   $F(1) + F(2) \in \mathcal{R}_3 = \{1, 2, 5, 6\}$ thus

   $F(2) \in F(0) + \mathcal{R}_1 \cap F(1) + \mathcal{R}_3 = \{3, 7\}$
3. $F(0) + F(3) \in \mathcal{R}_3 = \{1, 2, 5, 6\}$ and
   $F(1) + F(3) \in \mathcal{R}_2 = \{2, 3, 6, 7\}$ and
   $F(2) + F(3) \in \mathcal{R}_1 = \{1, 3, 5, 7\}$ thus

   $F(3) \in \{2, 6\}$ (**OR** $\{2, 6\}$)
4. $F(0) + F(4) \in \mathcal{R}_4 = \{4, 5, 6, 7\}$ and
   $F(1) + F(4) \in \mathcal{R}_5 = \{1, 3, 4, 6\}$ and
   $F(2) + F(4) \in \mathcal{R}_6 = \{2, 3, 4, 5\}$ and
   $F(3) + F(4) \in \mathcal{R}_7 = \{1, 2, 4, 7\}$ thus

   $F(4) \in \{\emptyset\}$ **if** $F(2) = 3$ and $F(3) = 2$
   $F(4) \in \{7\}$ **if** $F(2) = 3$ and $F(3) = 6$
   $F(4) \in \{5\}$ **if** $F(2) = 7$ and $F(3) = 2$
   $F(4) \in \{\emptyset\}$ **if** $F(2) = 7$ and $F(3) = 6$

Example

$\mathbb{F}_2^3$

$$\mathcal{R}_i := \{j \mid \mathcal{D}(i,j) \neq 0\}$$

$\mathcal{D}$	0	1	2	3	4	5	6	7
0	8	.	.	.	.	.	.	.
1	.	2	.	2	.	2	.	2
2	.	.	2	2	.	.	2	2
3	.	2	2	.	.	2	2	.
4	.	.	.	.	2	2	2	2
5	.	2	.	2	2	.	2	.
6	.	.	2	2	2	2	.	.
7	.	2	2	.	2	.	.	2

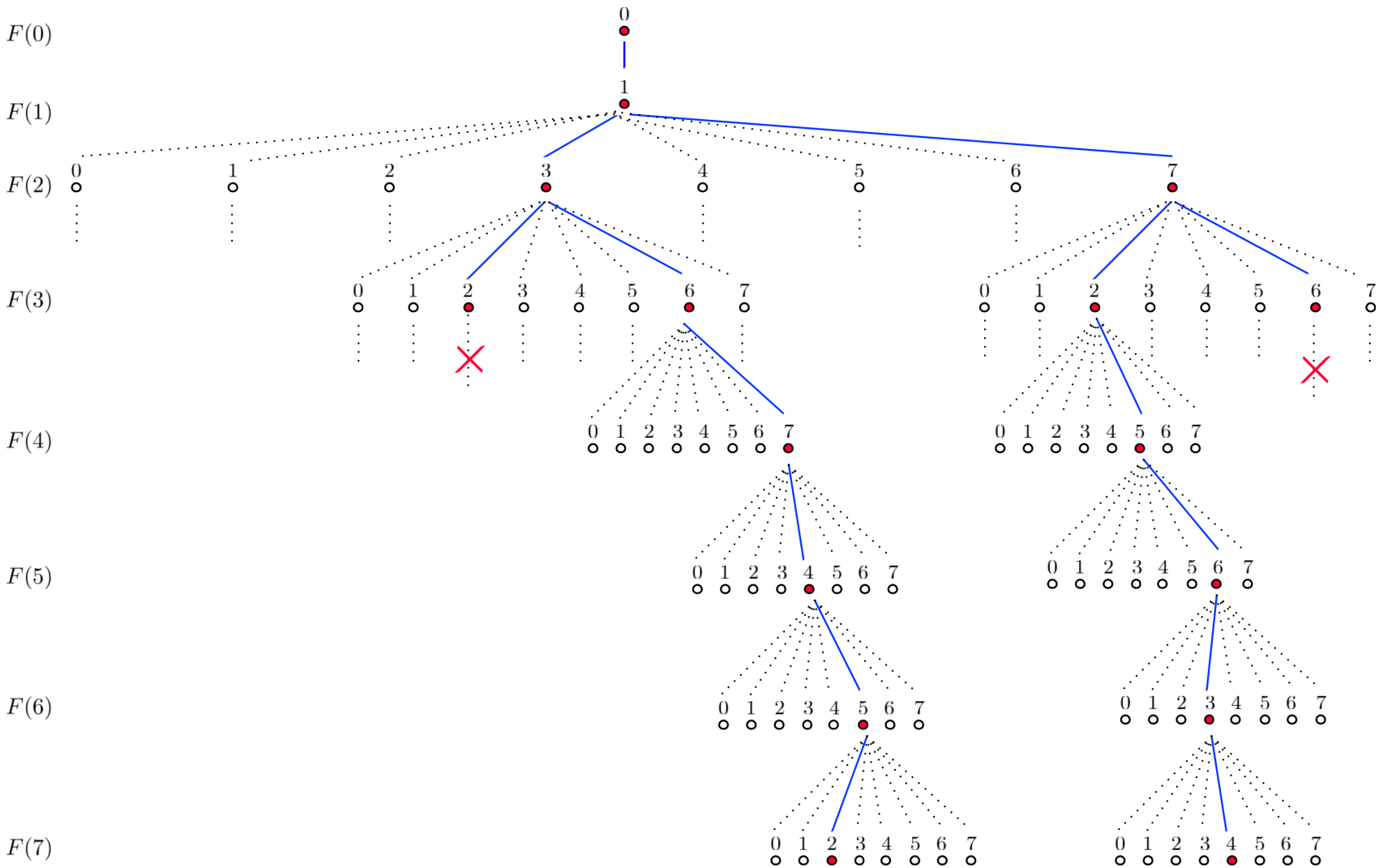
0. Set $F(0) = 0$
1. $F(0) + F(1) \in \mathcal{R}_1 = \{1, 3, 5, 7\}$
   Set $F(1) = 1$
2. $F(0) + F(2) \in \mathcal{R}_2 = \{2, 3, 6, 7\}$ and
   $F(1) + F(2) \in \mathcal{R}_3 = \{1, 2, 5, 6\}$ thus

   $F(2) \in F(0) + \mathcal{R}_1 \cap F(1) + \mathcal{R}_3 = \{3, 7\}$
3. $F(0) + F(3) \in \mathcal{R}_3 = \{1, 2, 5, 6\}$ and
   $F(1) + F(3) \in \mathcal{R}_2 = \{2, 3, 6, 7\}$ and
   $F(2) + F(3) \in \mathcal{R}_1 = \{1, 3, 5, 7\}$ thus

   $F(3) \in \{2, 6\}$ (**OR** $\{2, 6\}$)
4. $F(0) + F(4) \in \mathcal{R}_4 = \{4, 5, 6, 7\}$ and
   $F(1) + F(4) \in \mathcal{R}_5 = \{1, 3, 4, 6\}$ and
   $F(2) + F(4) \in \mathcal{R}_6 = \{2, 3, 4, 5\}$ and
   $F(3) + F(4) \in \mathcal{R}_7 = \{1, 2, 4, 7\}$ thus

   $F(4) \in \{\emptyset\}$ **if** $F(2) = 3$ and $F(3) = 2$
   $F(4) \in \{7\}$ **if** $F(2) = 3$ and $F(3) = 6$
   $F(4) \in \{5\}$ **if** $F(2) = 7$ and $F(3) = 2$
   $F(4) \in \{\emptyset\}$ **if** $F(2) = 7$ and $F(3) = 6$
5. $F(0) + F(5) \in \mathcal{R}_5 = \{1, 3, 4, 6\}$

   $\vdots$


$F(0)$
$F(1)$
$F(2)$
$F(3)$
$F(4)$
$F(5)$
$F(6)$
$F(7)$

Known functions

F and G are *trivial* if $F(x) \sim_{\mathcal{D}} G(x) = F(x + a) + b$

[Gorodilova'16] $\rightarrow$ (non-bijective) APNs with **non-trivial** γ-classes.

Known functions

F and G are *trivial* if $F(x) \sim_{\mathcal{D}} G(x) = F(x + a) + b$

[Gorodilova'16] $\rightarrow$ (non-bijective) APNs with **non-trivial** γ-classes.

What are the DDT-classes of '*optimal*' bijective SBoxes?

Known functions

F and G are *trivial* if $F(x) \sim_{\mathcal{D}} G(x) = F(x + a) + b$

[Gorodilova'16] $\rightarrow$ (non-bijective) APNs with **non-trivial** γ-classes.

What are the DDT-classes of '*optimal*' bijective SBoxes?

- $n = 6$: Dillon permutation $\rightarrow$ trivial DDT-class
- $n = 5$: five APN permutations $\rightarrow$ trivial DDT-classes
- $n = 4$: 16 4-differentially permutations $\rightarrow$ trivial DDT-classes
- $n = 3$: Gold permutation $(x \mapsto x^3) \rightarrow$ trivial DDT-class

Known functions

F and G are *trivial* if $F(x) \sim_{\mathcal{D}} G(x) = F(x + a) + b$

[Gorodilova'16] $\rightarrow$ (non-bijective) APNs with **non-trivial** γ-classes.

What are the DDT-classes of '*optimal*' bijective SBoxes?

- $n = 6$: Dillon permutation $\rightarrow$ trivial DDT-class
- $n = 5$: five APN permutations $\rightarrow$ trivial DDT-classes
- $n = 4$: 16 4-differentially permutations $\rightarrow$ trivial DDT-classes
- $n = 3$: Gold permutation $(x \mapsto x^3) \rightarrow$ trivial DDT-class

Question: Are DDT-classes for permutations *always* trivial? **NO**

Known functions and conjecture

F and G are *trivial* if $F(x) \sim_{\mathcal{D}} G(x) = F(x + a) + b$

[Gorodilova'16] $\rightarrow$ (non-bijective) APNs with **non-trivial** γ-classes.

What are the DDT-classes of '*optimal*' bijective SBoxes?

- $n = 6$: Dillon permutation $\rightarrow$ trivial DDT-class
- $n = 5$: five APN permutations $\rightarrow$ trivial DDT-classes
- $n = 4$: 16 4-differentially permutations $\rightarrow$ trivial DDT-classes
- $n = 3$: Gold permutation $(x \mapsto x^3) \rightarrow$ trivial DDT-class

Question: Are DDT-classes for permutations *always* trivial? **NO**
Question: Are DDT-classes of non-permutations *never* trivial? **NO**

Known functions and conjecture

F and G are *trivial* if $F(x) \sim_{\mathcal{D}} G(x) = F(x + a) + b$

[Gorodilova'16] $\rightarrow$ (non-bijective) APNs with **non-trivial** γ-classes.

What are the DDT-classes of '*optimal*' bijective SBoxes?

- $n = 6$: Dillon permutation $\rightarrow$ trivial DDT-class
- $n = 5$: five APN permutations $\rightarrow$ trivial DDT-classes
- $n = 4$: 16 4-differentially permutations $\rightarrow$ trivial DDT-classes
- $n = 3$: Gold permutation $(x \mapsto x^3) \rightarrow$ trivial DDT-class

Question: Are DDT-classes for permutations *always* trivial? **NO**
Question: Are DDT-classes of non-permutations *never* trivial? **NO**

Conjecture

For a bijective function,
the **rows** of its DDT are al distinct $\Rightarrow$ its **DDT-class** is trivial.

Bijective APN functions and their DDTs

Theorem

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a **bijective APN function**
Then, the rows of its DDT are pairwise distinct.

(the image sets of the derivatives of F are pairwise distinct.)

Proof Idea: by contradiction. We suppose two rows match, and then by induction on the images of the derivatives, we show that F is either not APN, or not a permutation.

Bijective APN functions and their DDTs

Theorem

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a **bijective APN function**
Then, the rows of its DDT are pairwise distinct.

(the image sets of the derivatives of F are pairwise distinct.)

Proof Idea: by contradiction. We suppose two rows match, and then by induction on the images of the derivatives, we show that F is either not APN, or not a permutation.

(!!) if the conjecture is **true**, DDT-classes of APN permutations are always **trivial**.

Outline

Introduction
- Symmetric cryptography
- Differentiality
- Equivalences

Results
- Equivalences
- Main contributions
- First Step for a classification
- Algorithm
- Experimental Results
- Special case

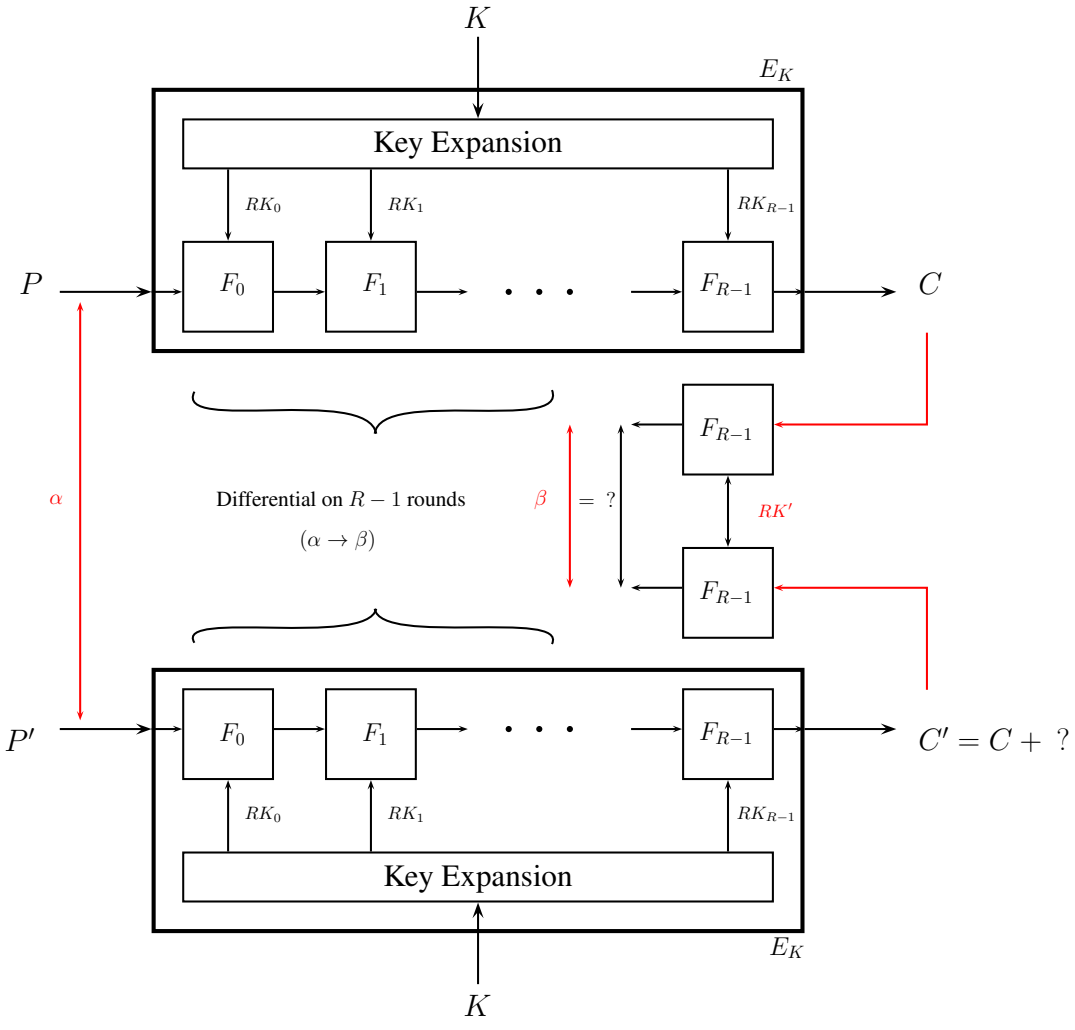
Conclusion

- **Contributions:**
  - Characterize and extend [Gorodilova'16] equivalence
  - an algorithm that computes classes
  - a new property about APN permutations
  - a conjecture on what are the functions with non-trivial classes

    ...
- **Future works:**
  - ... prove the conjecture ('*easier*' cases, e.g. quadratic APN)
  - what does it mean for a function to have derivatives with the same image set?
  - what are '*possible*' DDTs? (use and improve the algorithm)

C. Boura, A. Canteaut, J. Jean and V. Suder,
Two Notions of Differential Equivalence on SBoxes,
DCC, Design, Codes and Cryptography, To appear.

Differential Cryptanalysis of the last round



1. Encrypt N pairs P, $P' = P + \alpha$
2. For each pairs, decrypt the last round with RK'
3. Increment a counter if difference is β
4. Check which counter is the higher (closer from $N \times \mathbb{P}$)

Eli Biham and Adi Shamir,
Differential Cryptanalysis of DES-like Cryptosystems,
J. Cryptology 4(1), 1991.